

ZILKA-KOTAB

PC
ZILKA, KOTAB & FEECE™RECEIVED
CENTRAL FAX CENTER

JUN 28 2005

95 SOUTH MARKET ST. STE 420
SAN JOSE, CA 95113TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date: June 28, 2005	Phone Number	Fax Number
To: Patent Appeal Briefs, USPTO		(703) 872-9306
From: Kevin J. Zilka		

Docket No: NAIIP093/02.012.01App. No: 10/071,586

Total Number of Pages Being Transmitted, Including Cover Sheet: 30

Message:

Please deliver to the Appeal Brief division for Patents.

Thank you,

Kevin J. Zilka

RECEIVED
OIPE/IAP

JUN 29 2005

☐ Original to follow Via Regular Mail ☒ Original will Not be Sent ☐ Original will follow Via Overnight Courier

The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

June 28, 2005

RECEIVED
CENTRAL FAX CENTER

JUN 28 2005

Practitioner's Docket No. NAI1P093/01.012.01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Pantuso et al.

Application No.: 10/071,586

Group No.: 2137

Filed: 02/08/2002

Examiner: Callahan, Paul

For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A FIREWALL
SUMMARY INTERFACE

Mail Stop Appeal Briefs - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION-37 C.F.R. § 1.192)

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on April 28, 2005.
2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

*(When using Express Mail, the Express Mail label number is mandatory;
Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

with sufficient postage as first class mail.

37 C.F.R. § 1.10*

as "Express Mail Post Office to Addressee"

Mailing Label No. _____ (mandatory)

TRANSMISSION

facsimile transmitted to the Patent and Trademark Office, (703) 872-9306.

Date:

6/28/05

Signature

Jamie L. Rossi

(type or print name of person certifying)

* Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

Transmittal of Appeal Brief-page 1 of 2

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity \$500.00

Appeal Brief fee due \$500.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee \$500.00
Extension fee (if any) \$0.00

TOTAL FEE DUE \$500.00

6. FEE PAYMENT

Authorization is hereby made to charge the amount of \$500.00 to Deposit Account No. 50-1351 (Order No. NAI1P093).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P093).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Transmittal of Appeal Brief—page 2 of 2



Practitioner's Docket No. NAI1P093/01.012.01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Pantuso et al.

PATENT
RECEIVED
CENTRAL FAX CENTER

JUN 28 2005

Application No.: 10/071,586

Group No.: 2137

Filed: 02/08/2002

Examiner: Callahan, Paul

For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A FIREWALL
SUMMARY INTERFACE

Mail Stop Appeal Briefs - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION-37 C.F.R. § 1.192)

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on April 28, 2005.
2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory;
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

with sufficient postage as first class mail.

37 C.F.R. § 1.10*

as "Express Mail Post Office to Addressee"

Mailing Label No. (mandatory)

TRANSMISSION

facsimile transmitted to the Patent and Trademark Office, (703) 872-9306.

Date: 6/28/05

Signature

Jamie L. Rossi

(type or print name of person certifying)

* Only the date of filing (* 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under * 1.8 continues to be taken into account in determining timeliness. See * 1.703(f). Consider "Express Mail Post Office to Addressee" (* 1.10) or facsimile transmission (* 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

Transmittal of Appeal Brief--page 1 of 2

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity \$500.00

Appeal Brief fee due \$500.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee \$500.00
Extension fee (if any) \$0.00

TOTAL FEE DUE \$500.00

6. FEE PAYMENT

Authorization is hereby made to charge the amount of \$500.00 to Deposit Account No. 50-1351 (Order No. NAI1P093).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P093).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Transmittal of Appeal Brief—page 2 of 2

RECEIVED
CENTRAL FAX CENTER

JUN 28 2005

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of)
Pantuso) Group Art Unit: 2137
Application No. 10/071,586) Examiner: Callahan, Paul
Filed: February 8, 2002) Docket No. NAI1P093_02.012.01
For: SYSTEM, METHOD AND)
COMPUTER PROGRAM PRODUCT FOR) Date: June 28, 2005
A FIREWALL SUMMARY INTERFACE)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences**APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on April 28, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES
- III STATUS OF CLAIMS
- IV STATUS OF AMENDMENTS

NAI1P093_02.012.01

-1-

10071586

06/30/2005 WABDELRI 00000066 501351

500.00 DA

01 FC:1402

- V SUMMARY OF CLAIMED SUBJECT MATTER
- VI ISSUES
- VII ARGUMENTS
- VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL
- IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c))
(1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-12, 19-21 and 24

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-12, 19-21 and 24
3. Claims allowed: None
4. Claims rejected: 1-12, 19-21 and 24

C. CLAIMS ON APPEAL

The claims on appeal are: 1-12, 19-21 and 24

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

NAIIP093_02.012.01

-6-

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1 et al., as shown in Figures 3, 6A and 6B (and the related descriptions in the specification), a method for summarizing firewall activity is provided, including various operations such as: organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories, tracking a number of occurrences of each type of event utilizing the firewall and displaying a graphical representation indicating a severity of the number of the events utilizing the firewall. The graphical representation includes a graph. In addition, a selector is displayed for setting a blocking level of the firewall to a desired blocking level (e.g. item 602 of Figure 6A). Further, a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface (e.g. item 306 of Figure 3 et al.). Upon the selection of the summary interface, a recent activity list is displayed including total blocked access attempts by remote computers (e.g. item 310 of Figure 3). Upon the selection of the IP address interface, the IP address interface is displayed for selecting the IP addresses associated with the remote computers to be blocked (e.g. item 316 of Figure 3). Still yet, upon the selection of the event log, a log of the blocked access attempts by the remote computers is displayed (e.g. item 318 of Figure 3). Upon the selection of the notification option interface, a plurality of notification options is displayed for selection. Furthermore, a lock-down option is provided for selectively blocking all access attempts via an interface. Still yet, a user is capable of performing a visual trace (e.g. item 624 of Figure 6A), selectively blocking Internet control message protocol (ICMP) traffic, selecting the IP addresses associated with the remote computers to be allowed access, and selecting a list of application programs to be allowed to communicate over a network.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-12, 19-21 and 24 under 35 U.S.C. 103(a) as being unpatentable over Dick et al., U.S. Patent Application Publication No. 2002/0174340, in view of Schlossberg et al., U.S. Patent Application Publication No. 2002/0066034.

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

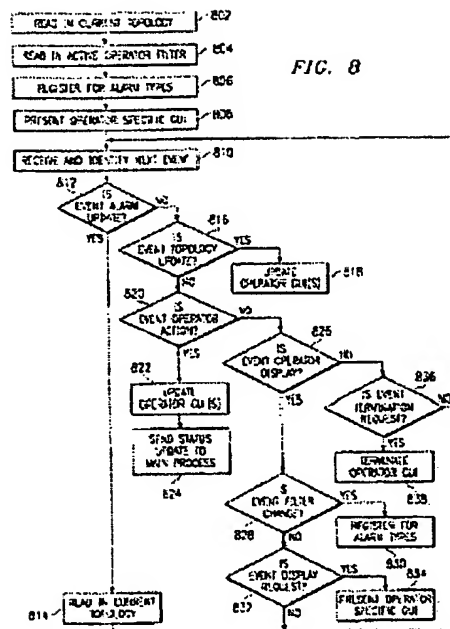
The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 1-12, 19-21 and 24 under 35 U.S.C. 103(a) as being unpatentable over Dick et al., U.S. Patent Application Publication No. 2002/0174340, in view of Schlossberg et al., U.S. Patent Application Publication No. 2002/0066034.

Group #1: Claims 1-8, 19-21 and 24

Specifically, with respect to each of the independent claims, the Examiner has cited the following figure from Krishnaswamy (USPN 5,867,494) to meet the abundant graphical user interface-related limitations in each of such claims.



However, such excerpt, as well as the remaining Krishnaswamy reference, is clearly lacking. Just by way of example, see the following emphasized limitations below which are present, at least in part, in each of the independent claims, but which are not met by any of the references relied on by the Examiner.

“wherein the graphical representation includes a graph;
wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;
wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:
upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,
upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and
upon the selection of the notification option interface, displaying a plurality of notification options for selection; wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
wherein a user is capable of performing a visual trace;
wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;
wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;
wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network."

Such novel combination of limitations is deemed to provide an enhanced firewall system.

It is noted that the Examiner has admitted that Dick and Schlossberg do not specifically mandate that the attempts may be seen via summary pages or pages for specific types of illicit access attempts. Despite such admission, the Examiner continues to invoke Official Notice that it is old and well-known to provide graphical user interfaces that give different viewing options for data, etc. To support such Official Notice assertion, the Examiner has cited Figure 8 from Krishnaswamy above. As noted above, however, such except and the remaining Krishnaswamy reference do not meet such claim limitations, contrary to the Examiner's assertion.

To this end, the Examiner has not still not satisfactorily satisfied appellant's request for a specific showing of ALL of the subject matter in ALL of the claims. Note excerpt from MPEP below.

"If the appellant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. In re Vaack, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Dick and Schlossberg fail to teach all of appellant's claim limitations, as noted above.

Group #2: Claim 9

With respect to Claim 9, the Examiner has stated that appellant's claimed interface "wherein the first type of the blocked attempts, the second type of the blocked attempts, and the third type of the blocked attempts are organized into categories" is obvious because of "Dick's logging."

However, Dick only teaches that "[c]ommon features of firewall include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall" ([0065]). Clearly the mere mention of a firewall that logs does not meet appellant's specific claim language since appellant specifically claims organizing blocked attempts into categories.

Again, appellant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Dick and Schlossberg fail to teach all of appellant's claim limitations, as noted above.

Group #3: Claims 10-12

With respect to Claims 10-12, the Examiner has stated that appellant's claimed interface "wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith" (Claim 10), "wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith" (Claim 11), and "wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith" (Claim 12) are rendered obvious by Schlossberg's monitoring of the attacker.

Appellant respectfully asserts that simply monitoring an attacker does not meet appellant's claimed "displaying," especially not in the specific manner claimed by appellant as quoted above.

Again, appellant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Dick and Schlossberg fail to teach all of appellant's claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for summarizing firewall activity, comprising:
 - (a) organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
 - (b) tracking a number of occurrences of each type of event utilizing the firewall; and
 - (c) displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

2. (Original) The method as recited in claim 1, wherein the events include blocked attempts of various types.
3. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers to access predetermined banned ports associated with the local computer.
4. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of IP addresses to access the local computer.
5. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts to access the network made by predetermined applications.
6. (Previously Presented) The method as recited in claim 1, wherein the displayed number of occurrences of each type of event occurred within a predetermined time period.
7. (Previously Presented) The method as recited in claim 1, and further comprising displaying additional information relating to the events upon the selection thereof.

8. (Previously Presented) The method as recited in claim 2, wherein a first type of the blocked attempts includes blocked attempts of the remote computers to access predetermined banned ports associated with the local computer, a second type of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of IP addresses to access the local computer, and a third type of the blocked attempts includes blocked attempts to access the network made by predetermined applications.
9. (Previously Presented) The method as recited in claim 8, wherein the first type of the blocked attempts, the second type of the blocked attempts, and the third type of the blocked attempts are organized into the categories.
10. (Original) The method as recited in claim 8, wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith.
11. (Original) The method as recited in claim 8, wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith.
12. (Original) The method as recited in claim 8, wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith.
13. - 18. (Cancelled)
19. (Previously Presented) A computer program product embodied on a computer readable medium for summarizing firewall activity, comprising:
 - (a) computer code for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;

- (b) computer code for tracking a number of occurrences of each type of event utilizing the firewall; and
- (c) computer code for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;
 - wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;
 - wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:
 - upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,
 - upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,
 - upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and
 - upon the selection of the notification option interface, displaying a plurality of notification options for selection;
 - wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
 - wherein a user is capable of performing a visual trace;
 - wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;
 - wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;
 - wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

20. (Previously Presented) A system for summarizing firewall activity, comprising:

- (a) logic for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
- (b) logic for tracking a number of occurrences of each type of event utilizing the firewall; and
- (c) logic for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

21 (Previously Presented) A system for summarizing firewall activity, comprising:

- (a) means for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
- (b) means for tracking a number of occurrences of each type of event utilizing the firewall; and
- (c) means for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

22. – 23. (Cancelled)

24. (Previously Presented) A firewall method, comprising:

- (a) executing a firewall in association with a local computer;
- (b) identifying a number of blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer;
- (c) identifying a number of attempts of the remote computers to access predetermined frequently-used ports associated with the local computer;
- (d) identifying a number of blocked attempts to access a network made by predetermined applications on the local computer;
- (e) displaying a menu for selecting from a plurality of interface features including a summary page, an applications page, an event log, and an IP address page;
- (f) upon the selection of the summary page on the menu,
 - (i) displaying a recent activity list including recent activity icons corresponding to events including total blocked attempts, the attempts of the remote computers to access the predetermined frequently-used ports associated with the local computer, the blocked attempts of the remote computers with the predetermined set of IP addresses to access the local computer, the recent activity list further including a total number of the events within a predetermined time period corresponding with each recent activity icon, and a graphical representation indicating a severity of the total number of the events,
 - (ii) displaying a frequently accessed port list including port icons corresponding to the predetermined frequently-used ports, the frequently accessed port list further including a total number of the attempts corresponding with each predetermined frequently-used

- ports, and a graphical representation indicating a severity of the total number of the attempts,
- (iii) displaying a commonly blocked IP address list including IP address icons corresponding to banned IP addresses from which the blocked attempts of the remote computers occurred, the commonly blocked IP address list further including a total number of the blocked attempts corresponding with each IP address icon, and a graphical representation indicating a severity of the total number of the blocked attempts,
 - (iv) displaying a commonly blocked application list including application icons corresponding to banned applications associated with the blocked attempts, the commonly blocked application list further including a total number of the blocked attempts corresponding with each application icon, and a graphical representation indicating a severity of the total number of the blocked attempts;
- (g) upon the selection of the applications page on the menu, displaying an applications interface for selecting the predetermined applications;
 - (h) upon the selection of the untrusted IP address page on the menu, displaying an untrusted IP address interface for selecting the IP addresses associated with remote computers to be blocked; and
 - (i) upon the selection of the event log on the menu, displaying a log of the attempts;
 - wherein a slider bar is displayed for setting a blocking level of the firewall by sliding the slider bar to a desired blocking level;
 - wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
 - wherein a user is capable of performing a visual trace;
 - wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;
 - wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over the network.

25. – 26. (Cancelled)

**IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE
APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P093_02.012.01).

Respectfully submitted,

By: _____

Kevin J. Zilka

Reg. No. 41,429

Date: _____

6/28/05

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660